ハイライトレポート

2024. 8. 28 Day2

法規制対応が急務に！
IoT/OTデバイスに求められるセキュリティ対策とは
～CRAの最新動向と対策～

セキュリティ対策に乗り遅れないために

産業制御機器のIoT化と巧妙化するサイバー攻撃の脅威に備えるべく、早急なセキュリティ対策が求められています。2027年にはサイバーレジリエンス法の全面施行が予定されている等、サイバーセキュリティを義務とする法制化の動きも世界全体に広がりを見せています。ウェビナでは、サイバーセキュリティ対策のカギとなるIEC 62443から、法規制の対象とされる製品やソフトウェア・IC選び・脆弱性管理から構築すべきシステム要件まで、様々な情報とノウハウを厳選し、2Days・4セッションに渡って配信いたしました。

IoT/OTシステムの制約によるセキュリティ課題

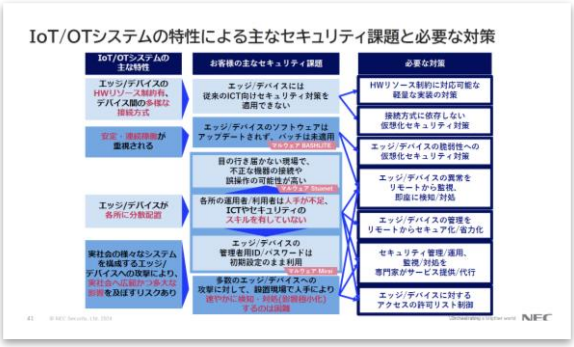
IoT/OT機器を狙ったサイバー攻撃は年々増加・多様化しています。しかし、従来のICT向けのセキュリティ対策は、大きなメモリ容量や高いCPU性能が必要となり、IoT/OT機器への適用はハードウェアの制約から困難です。またIoT/OT機器ならではのセキュリティ課題として以下の点が挙げられます。

・ソフトウェアがアップデートされず、パッチが適用されない
・分散配置されたデバイスのリモート管理、対応の自動化が求められる
・攻撃されたデバイスに留まらず、実社会へ広範な影響を及ぼすリスクがある

このような課題に対応するため、「**少ないHWリソースで実装可能な軽量さ**」、「**異常を即座に検知できるリアルタイム性**」、「**リモートでの集中管理**」といった機能が求められます。

■ 本日の登壇者 ■

NECセキュリティ株式会社
IoT/OTセキュリティユニット
ディレクタ（ユニット長）
桑田 雅彦　氏

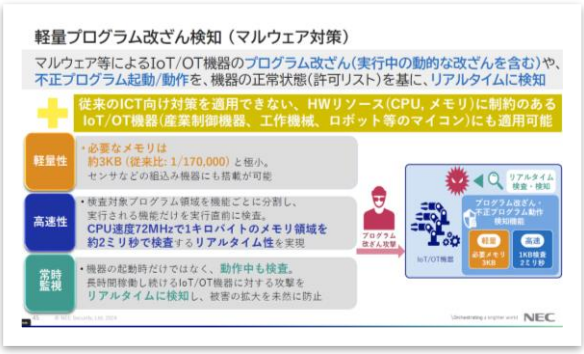


IoT/OTシステムの特性による主なセキュリティ課題と対策
出所：投影資料より一部抜粋

NECはIoT/OT向けセキュリティ対策を拡充中

NECは、IoT/OTの特性・制約に適用可能で自社の強み技術を活かした、新たなIoTセキュリティ製品を拡充し、提供中です。

■課題に対する製品例
・低性能のデバイスでも不正動作を防ぎたい …
⇒ キロバイト単位のメモリ容量でリアルタイムな不正動作検知が可能な「**軽量プログラム改ざん検知**」機能



軽量プログラム改ざん検知（マルウェア対策）
出所：投影資料より一部抜粋

・分散配置された大量のデバイスをリモート管理したい…
⇒ デバイスの認証情報（ID、暗号鍵、電子証明書）をリモートから簡単に自動配付/更新できる「**SecureWare/Credential Lifecycle Manager**」機能

セキュリティに関してお困りの方は是非お問い合わせください。

他記事、ウェビナ、お問い合わせはこちら

リョーサンテクラボ
エンジニアによりそうマガジンサイト